Just Gaze and Wave: Exploring the Use of Gaze and Gestures for Shoulder-surfing Resilient Authentication

Yasmeen Abdrabou[1,2], Mohamed Khamis[3], Rana Mohamed Eisa[4], Sherif Ismail[1], Amr Elmougy[4]
[1]German University in Cairo, Egypt, {firstname.lastname}@guc.edu.eg
[2]Bundeswehr University, Munich, Germany, yasmeen.abdrabou@unibw.de
[3]University of Glasgow, United Kingdom, Mohamed.Khamis@glasgow.ac.uk
[4]University of Canada in Egypt, Egypt, {firstname.lastname}@uofcanada.edu.eg

ABSTRACT

Eye-gaze and mid-air gestures are promising for resisting various types of side-channel attacks during authentication. However, to date, a comparison of the different authentication modalities is missing. We investigate multiple authentication mechanisms that leverage gestures, eye gaze, and a multimodal combination of them and study their resilience to shoulder surfing. To this end, we report on our implementation of three schemes and results from usability and security evaluations where we also experimented with fixed and randomized layouts. We found that the gaze-based approach outperforms the other schemes in terms of input time, error rate, perceived workload, and resistance to observation attacks, and that randomizing the layout does not improve observation resistance enough to warrant the reduced usability. Our work further underlines the significance of replicating previous eye tracking studies using today's sensors as we show significant improvement over similar previously introduced gaze-based authentication systems.

CCS CONCEPTS

• **Security and privacy**; • **Human-centered computing** → **Human computer interaction (HCI)**;

KEYWORDS

Multimodal Authentication, Mid-air Gestures, Authentication

ACM Reference Format:
Yasmeen Abdrabou[1,2], Mohamed Khamis[3], Rana Mohamed Eisa[4], Sherif Ismail[1], Amr Elmougy[4]. 2019. Just Gaze and Wave: Exploring the Use of Gaze and Gestures for Shoulder-surfing Resilient Authentication. In *2019 Symposium on Eye Tracking Research and Applications (ETRA '19), June 25–28, 2019, Denver , CO, USA*. ACM, New York, NY, USA, 10 pages. https://doi.org/10.1145/3314111.3319837

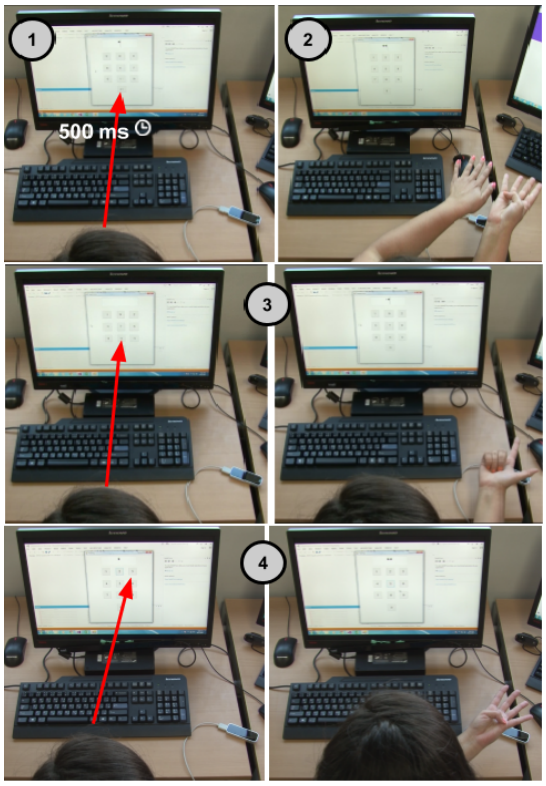


Figure 1: The figure shows a participant (1) authenticating using gaze by dwelling at 2 for 500 ms, (2) authenticating using gestures by extending 9 fingers, (3) authenticating using GazeGestures+Random where the user first gazes at the digit 4, which is displayed on a randomized layout, and then extends 2 right hand fingers resulting in an input of 4 + 2 = 6, (4) authenticating using GazeGestures by gazing at 6, which is displayed on a fixed layout, and then extends 4 left hand fingers resulting in an input of 6 − 4 = 2.

1 INTRODUCTION

With computers enabling ubiquitous access to private data, numerous authentication schemes have been proposed and adopted by users. Privacy-aware users employ graphical passwords, alphanumeric passwords, and PINs to protect access to their computers, online accounts, and sensitive files. However, many of these schemes are vulnerable to different types of side-channel attacks. For example, alphanumeric and graphical passwords are known to be vulnerable to shoulder surfing and video attacks [16, 29, 33]. A study conducted by the Ponemon Institute investigated shoulder surfing attacks in business office environments and found that 12% of observed content was login credentials (e.g., passwords) and that

ETRA '19, June 25–28, 2019, Denver , CO, USA

ACM ISBN 978-1-4503-6709-7/19/06…$15.00
https://doi.org/10.1145/3314111.3319837

91% of attacks were successful [20]. Other forms of side-channel attacks include thermal and smudge attacks, which can reveal passwords entered on keyboards and touchscreens [1, 5, 27].

Many smartphones come with a fingerprint reader integrated, and advances in depth cameras promise seamless integration of facial recognition in commodity devices (e.g., iPhone X). In addition to physiological biometrics, another promising area is behavioral biometrics [10, 11], in which behavior is used to identify the legitimate user. However, while biometric authentication schemes are not vulnerable to the aforementioned side-channel attacks, they come with different problems as they cannot be changed once leaked. Furthermore, they often result in third-parties learning about the user's biometric data, which can, in turn, be misused or stolen remotely [32, 39]. Therefore, designing secure knowledge-based schemes, i.e., schemes that require the legitimate user to *know* something such as a password, which resists these types of attacks is essential to fit different user preferences, tasks, and contexts.

At the same time, sensors such as eye trackers and motion sensors are increasingly becoming more accurate, affordable, and are already integrated into some consumer devices today. Previous work has shown that employing gaze [15, 24] and gestures [4, 18] can significantly improve authentication schemes in terms of observation resistance. Furthermore, the combination of multiple modalities can significantly complicate shoulder surfing attacks [8, 23] An additional advantage of at-a-distance interaction modalities, such as gaze or gestures, is that they allow designing schemes that split the shoulder surfer's attention to (1) the user's input, and (2) the screen. For example, to shoulder surf a user's gaze input in response to on-screen cues, the attacker would have to observe the user's eye movements, in addition to the on-screen cues [24].

While recent work compared multiple modalities for cue-based authentication [25], a comparison of multimodal authentication approaches is missing. To close this gap, we report on 6 concepts:

(1) **Gaze+Random:** Gaze-based Authentication with a randomized arrangement of on-screen digits.
(2) **Gaze-only:** Gaze-based Authentication with a fixed arrangement of on-screen digits.
(3) **Gestures-only:** Hand Gestures-based Authentication.
(4) **GazeGestures+Random:** Multimodal authentication using hand gestures and gaze with a randomized on-screen digits.
(5) **GazeGestures:** Multimodal authentication using hand gestures and gaze with a fixed arrangement of on-screen digits.
(6) **Baseline:** Traditional keyboard-based authentication.

In our gaze-based systems, users dwell at a digit on an on-screen number pad for 500 ms to select it. While in Gestures-only, the number of fingers the user extends denote the input. Finally, in the multimodal approaches, users authenticate by gazing at a digit on an on-screen number pad, then perform a hand-gesture to indicate an addition or subtraction operation to be applied on the gazed at digit. For example, to enter 5 the user could gaze at 2 and extend 3 right-hand fingers, or gaze at 6 and extend 1 left-hand finger. The multimodal approach was introduced to enhance the security in the Gestures-only modality.

While multimodal approaches are often superior to unimodal ones [7, 21], we found that the gaze-based approach outperforms the other schemes in terms of input time, error rate, perceived workload and resistance to shoulder surfing attacks. Multimodal GazeGestures were found to be highly resilient to shoulder surfing, but suffer from lower usability, hence we recommend them only when additional security is needed rather than for daily use. Although our gaze-based approach is a replication of a previous system proposed in 2007 [26], our study results indicate a significant (70%) improvement over prior work in authentication time mainly due to the use of better sensors and improved visual computing techniques. This motivates the replication of previous work.

2 RELATED WORK

Traditional PINs and alphanumeric passwords are among of the most commonly used authentication methods [36], yet they are vulnerable to several types of side channel attacks. A widely studied side channel attack is shoulder surfing, where a malicious attacker attempts to observe the user during authentication, in order to later gain access to the user's device [16]. Previous work also explored smudge attacks against touchscreens. In a smudge attack, the attacker examines the device's touchscreen and tries to find the entered PIN or graphical password based on the oily residues left after entering the password [5]. Traditional password input methods are also vulnerable to thermal attacks, in which an attacker employs a thermal camera to detect the heat traces resulting from the user's interaction with the device to eventually infer the password [1, 27].

A challenge in this field is to design methods that are easy to use, efficient and effective from a usability perspective, while at the same time maintaining high security. Prior work proposed a variety of, mostly individual, interaction techniques to protect against the aforementioned attacks. In our work, we compare and evaluate the usability and security of multiple unimodal and multimodal authentication schemes. In the following, we discuss prior work that investigated similar authentication modalities.

2.1 Authentication using Gaze

Humans move their eyes quickly. Additionally, while eye movements are overt, the resolution of gaze interfaces can be designed to encourage covert eye movements that are challenging to observe. This inspired researchers to leverage eye gaze for authentication. One of the leading efforts in eye-Gaze authentication was proposed by De Luca et al. who introduced and compared several gaze-based authentication schemes [14], one of which was referred to as EyePIN in a follow-up project [9]. Users authenticate using EyePIN by gazing at digits on an on-screen number pad; selection occurs after a dwell time of 800 ms. Later, De Luca et al. introduced EyePassShapes, which relies on a series of gaze gestures [9]. EyePassShapes required more time (12.5 seconds) but was assumed to be more secure since it is more difficult to observe multiple consecutive gaze gestures. Kumar et al. proposed EyePassword, an authentication scheme that combines gaze with keyboard input; users gaze at a digit on an on-screen keyboard and then select it either by dwell time or by pressing the space bar on their physical keyboard [26]. CGP is a cued-recall graphical password with a larger password space, where users can recall several distinct passwords [17]; its users authenticate by looking at certain positions on a given picture. Finally, several works proposed gaze-based behavioral biometric authentication [30, 31].

2.2 Authentication using Gestures

Similar to gaze, mid-air gestures were investigated for knowledge-based authentication (i.e., by providing a password) and for biometric authentication. George et al. evaluated a mid-air version of Android patterns for immersive virtual environments, where a user wears a Head-mounted Display and draws a pattern on a virtual 3×3 grid using a handheld controller [18]. Hayashi et al. proposed biometric authentication using gestural patterns and body segments [19]. Aslan et al. exploited individual differences among users in performing mid-air gestures for biometric authentication [3].

2.3 Multimodal Authentication

Researchers have studied how to utilize multiple modalities to combat shoulder surfing. Bianchi et al. proposed multiple authentication schemes: SpinLock, ColorLock and Phone Lock, in which PIN entry on mobile devices is guided by haptic or audio cues [6–8]. Here, users hear audio cues or perceive vibrations, and accordingly, they modify their input. Although their security was not formally evaluated, they are expected to be more secure than traditional PIN entry since attackers would have to observe the cue, and the user's input in response to the cue to eavesdrop the password.

In these works, the additional modality was an output modality (haptic or audio) to support users in providing PINs using an input modality (touch). On the other hand, a body of work explored using multiple *input* modalities; GazeTouchPass and GazeTouchPIN allow users to authenticate on mobile devices using touch input and gaze input [21, 24], while GTmoPass is an adaptation of GazeTouchPass for public display scenarios [23]. In GazeTouchPass, users authenticate by providing a multimodal password consisting of digits entered via touch and gaze gestures detected by the front-facing camera of the mobile device (e.g., touch(1), gaze(left), touch(2), gaze(right)). While in GazeTouchPIN, users first tap a pair of digits, and then gaze left or right to specify which digit they want to enter. The layout of the shown digits is randomly determined based on one of two predefined layouts. This means that observing the gaze input in an occasion, and the touch input in another occasion, and then combining the observations is very unlikely to reveal the password. Overall, these systems demonstrated higher resistance to shoulder surfing at the expense of longer authentication times. For example, combining gaze and touch input made authentication highly secure against observations, but mean authentication times were 3.1 seconds [21], and 10.8 seconds [24].

We employ a similar implementation of EyePIN [9], with a slightly shorter dwell duration (500 ms instead of 800 ms). However, in our study, participants authenticated in 5.3 s, while EyePIN users authenticated in 13 s. For gestures, we explore authentication by extending a number of fingers, which was not studied before. Finally, we explore multimodal authentication using mid-air gestures and gaze, which were never employed for authentication before. We previously presented our concepts as a poster [2]; we significantly extend this by in-depth evaluation and discussion of their implementation, usability and security.

3 CONCEPT AND IMPLEMENTATION

In this section, we describe the concepts that we explored for authentication, as well as their implementation.

3.1 Gaze-based Authentication

Gaze is subtle yet intuitive, making it a promising modality to employ when susceptible to shoulder surfing. As we discussed in section 2.1, gaze has been leveraged for authentication before.

In our system implementation, we use a similar layout to that of EyePIN [14]. The difference is our users authenticate using our system by fixating their eyes on the desired digit for 500 ms. For example, to select 2 in Figure 1.1, the user should dwell on the digit for 500 ms. The dwell time was decided based on a pilot test where we compared three dwell times from prior work in eye tracking [9, 17], and had participants try them and provide feedback. 500ms was deemed natural and induced few errors.

In our implementation, calibration is essential at the beginning. However, advances in visual computing promise either a significant reduction of calibration time [28] or a complete elimination of calibration by, for example, appearance-based gaze estimation methods [38]. Hence we expect that future systems would require marginal time for calibration.

In Gaze-only, we show the user a classical 10-digit number pad. However, in Gaze+Random, the order of digits is randomized. Adding randomness results in higher observation-resistance, because it would require the attacker to observe both: (1) the user's gaze input, and (2) the layout to which the user is reacting. On the downside, a random arrangement of digits would likely result in longer entry times since users would need to perform a linear search to find the desired digit. It could also increase the error rate.

Whenever input was detected, the system made a "button clicked" sound to indicate that an entry has been recognized. A password field was updated at each entry. The password field was designed to be large enough for users to notice that it has been updated in their periphery. These two features, as well as the dimensions of the layout, were determined based on a pilot test with 3 participants.

3.2 Gesture-based Authentication

While it might be obvious to observers, signaling digits via hand fingers is likely to be highly intuitive. It also could be less secure, that's why we added the multimodal approach discussed in subsection 3.3 to be able to compare the modalities at the end and to enhance the gesture-based security.

In our implementation of Gestures-only, the user performs a hand gesture to signal the desired digit in the area above a leap motion sensor, which we use for gesture recognition. The sensor counts the number of fingers extended for one second to determine the intended digit. This threshold was essential to prevent unintentionally inputting zero when changing from one digit to another. Users can use either hands or both of them to indicate the digit. Figure 1.2, shows an example of a user entering digit 9 by both of her hands. In case of input via gestures, the interface shows an additional entry in the password field.

3.3 Multimodal Gaze and Gestures

The multimodal approach combines both, the user's gaze and the performed gestures in one authentication method. This method was introduced as a way to make the Gestures-only authentication more secure. First, the user gazes at an on-screen digit and then performs a mid-air gesture by extending a number of fingers above

the Leap Motion. Using right-hand fingers results in adding the gesture-based input to the gaze-based input, while the left-hand fingers result in a subtraction.

Figures 1.3 left and 1.3 right, show an example where the user gazed at the digit 4 and extended 2 right-hand fingers, hence the entered digits are 4 + 2 = 6. On the other hand, Figures 1.4 left and 1.4 right, show an example of a user gazing at 6 and extending 4 left-hand fingers, so the entered digit is 6 - 4 = 2. The system awaited input using both modalities. This means that gazing at the correct digit would only activate it if the leap motion can detect a hand without any fingers extended. This method is complicated than the previous ones as it needs basic math calculation in each digit entry, which will put an extra delay on the authentication time; however, it is expected to be more secure.

We refer to this system as GazeGestures. Similar to gaze-based authentication (Section 3.1), we implemented a version of GazeGestures with a randomized on-screen arrangement of digits, and a version with a fixed layout.

4 USABILITY STUDY EVALUATION

The goal of this study was to collect a realistic set of login attempts to analyze usability, as well as video recordings to be used in the security evaluation.

4.1 Experimental Design

The study was designed as a within-subjects repeated measures experiment; i.e., all participants went through all conditions. The study involved one independent variable: the authentication method. Our experiment covered six conditions: (1) Gaze-only with Random Layout, (2) Gaze-only with Fixed Layout, (3) Gestures-only, (4) GazeGestures with random layout, (5) GazeGestures with fixed layout, and (6) PIN (baseline).

4.2 Dependent Variables and Hypotheses

We measured the effect of the six authentication methods on:

- Entry time: starting from the moment the password is told to the user, until the moment the password is recognized by the system.
- Error rate: the number of times the password was entered incorrectly before successfully authenticating. An entry was considered to be an error if one or more of the password's symbols were incorrect.
- Perceived workload: through the NASA-TLX questionnaire.
- Subjective feedback: collected through a questionnaire and a semi-structured interview.

The following are the null hypotheses:

$H_{0,0}$ There is no statistically significant relationship between the authentication method and entry time.

$H_{0,1}$ There is no statistically significant relationship between the authentication method and error rate.

4.3 Apparatus and Participants

To detect the gestures, we used a Leap Motion Model lm-c01[1]. It was placed on the right-hand side for right-handed participants, and on the left-hand side for left-handed participants. We made sure it does not result in the user's hand obstructing the eye tracker's view. The recognition range of the used Leap Motion is between 82.5 mm and 317.5 mm. Gaze input was detected using a Tobii 4C eye tracker (60 Hz) [2]. The eye tracker was attached to a monitor (17", 1366 × 768 pixels). The sensors were set up as illustrated in Figure 2. We built a CSharp interface in Visual Studio 2012 with the use of the Tobii and Leap Motion SDKs. Participants were free to enter the baseline PINs using the keyboard or the mouse. Participants sat 80 cm away from the display. We video recorded participants during the study using an HD video camera from the back, that shows the gesture input and screen layout, and a webcam from the front, that shows the user's gaze input. The cameras were positioned in a way to simulate an attacker that is observing the user.

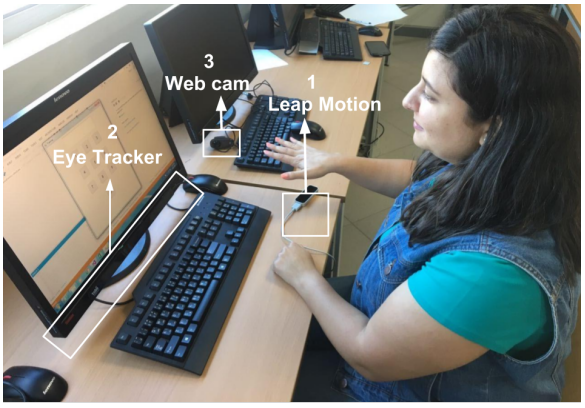


Figure 2: The Usability study setup consisted of 1) a Leap Motion to detect extended fingers, 2) Tobii eye tracker for gaze input, 3) a web cam and an HD camera to record the user while authenticating for follow up security analysis.

We invited 17 participants aged between 21 and 28 (Mean=24.41; SD=1.87), four of them wear glasses. Ten of which were males and seven were females. Participants came from a variety of backgrounds including students and teaching assistants from engineering, computer science, business informatics majors.

4.4 Experiment Procedure

After arriving at our lab, participants filled-in a consent form. The experimenter then explained the study and collected the participant's demographics. After that, the eye tracker was calibrated for the participants using Tobii's software. Each participant then went through 6 blocks, each block covered one condition. The order of blocks was counterbalanced using a Latin Square. Blocks that involved GazeGestures and GazeGestures+Random were divided into 5 stages, the rest were divided into 4 stages. In Stage 1, participants performed 2 training runs using the respective condition to get acquainted with the authentication method. In Stage 2, participants performed 5 authentications using the current block's authentication method. We limited Stage 2âĂŹs authentications to 5 to reduce the likelihood of eye fatigue and maintain a reasonable experiment duration; in real authentication scenarios, users would not authenticate as often as they did in our study. The required

[1] https://www.leapmotion.com/

[2] https://tobiigaming.com/eye-tracker-4c/

passwords were different in each stage and were read out loud by the experimenter according to a random predefined list. After each successful login, an "access granted" message was shown, and then the participant was asked to proceed enter the following password. If the wrong password is detected an error message was shown instead, and the user had to reattempt entry until successful.

For realism and to measure the error rate, participants were able to reenter incorrectly detected passwords. In the case of GazeGestures, the participant was free to choose the digits to gaze at and the gestures to perform in order to enter the intended password.

For example, to enter 5, a participant could gaze at the digit 3 and add 2 using a right-hand gesture, or gaze at 9 and subtract 4 using a left-hand gesture. These entries were then analyzed to evaluate the usability of the method. To understand the participants' PIN choices using our methods, the participant was asked to choose his/her own PIN in Stage 3. The participant entered the chosen PIN two consecutive times as done on typical authentication systems: users need to confirm the password they have created to aid memorability and overcome entry errors. For instance, would users gaze at the same digit and perform the same gesture when using GazeGestures, or would they provide the digit in different ways every time? In both conditions that involve GazeGestures, participants went through an additional stage. In Stage 4, participants entered the same password they defined in the previous stage, but this time with the system telling the user which hand to use for performing the gestures. This was done to understand how users feel about restrictions (e.g., password policies) intended to strengthen their password entry. In the final stage, participants filled in a questionnaire in which we asked for their subjective feedback regarding the block's method, and they filled in a NASA TLX questionnaire.

4.5 Limitations

One limitation of the usability study is that three participants reported experiencing eye fatigue after authenticating via eye gaze several times. This happened in cases where Gaze-only and Gaze + Random blocks came directly after each other. Note, however, that users authenticated multiple consecutive times for our experimentation purposes, and that in realistic scenarios, they are likely to authenticate significantly fewer times.

4.6 Usability Experiment Results

Prior to analyzing the entry time and error rate, we excluded the data from 2 out of 17 participants due to technical problems.

4.6.1 Entry time. The authentication in time in seconds can be seen in figure 3. In addition, a repeated measures ANOVA with Greenhouse-Geisser correction revealed a significant main effect of the authentication method on entry time $F_{1.5,20.93} = 26.2$, $p < 0.001$; thereby disproving null hypothesis $H_{0,0}$. Pairwise comparisons with Bonferroni correction showed significant differences between multiple pairs (see Table 1).

The results show that authenticating using the baseline is significantly faster than all other methods. Gaze-only and Gaze+Random come second, being significantly faster to authenticate with compared to the remaining methods. Gaze-only is slightly faster than Gaze+Random, however, the difference is not significant ($p > 0.05$). Gestures-only is significantly faster than GazeGestures and GazeGestures+Random. Finally, the difference between GazeGestures and GazeGestures+Random is not significant ($p > 0.05$).

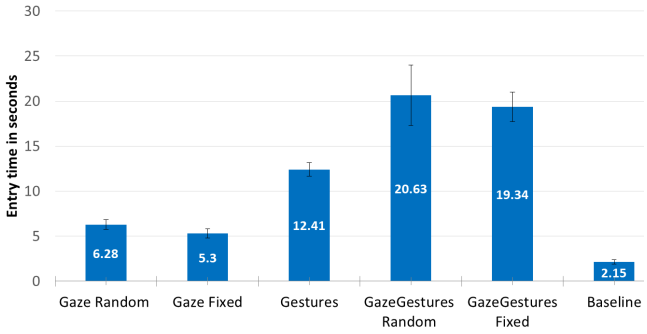
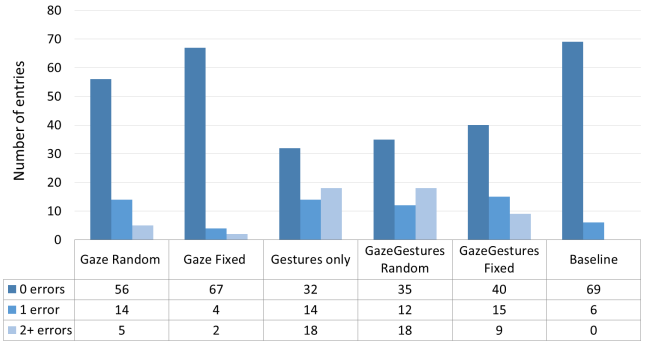


Figure 3: Authentication time in seconds. The gaze methods are faster to use compared to Gestures and GazeGestures.



	Gaze Random	Gaze Fixed	Gestures only	GazeGestures Random	GazeGestures Fixed	Baseline
0 errors	56	67	32	35	40	69
1 error	14	4	14	12	15	6
2+ errors	5	2	18	18	9	0

Figure 4: The number of attempts before a successful entry. Baseline and Gaze-only are the least error-prone. Gaze+Random is slightly more error-prone.

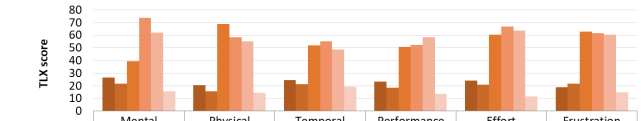
4.6.2 Error Rate. A repeated measures ANOVA with Greenhouse-Geisser correction revealed a significant main effect of the authentication method on error rate $F_{1.97,27.53} = 4.9$, $p < 0.05$; thereby disproving null hypothesis $H_{0,1}$. Pairwise comparisons with Bonferroni correction revealed significant differences between some pairs. Namely, the Baseline ($M = 0.08$, $SD = 0.04$) is significantly less error-prone compared to GazeGestures ($M = 1.16$, $SD = 0.23$) and GazeGestures+Random ($M = 1.69$, $SD = 0.27$). Similarly, Gaze-only ($M = 0.25$, $SD = 0.17$) is significantly less error-prone compared to GazeGestures and GazeGestures+Random. Figure 4 illustrates the number of attempts before a successful entry.

4.6.3 Perceived Workload. Figure 5 illustrates the responses to the NASA TLX. In general, Baseline, Gaze-only, and Gaze+Random were the least demanding. Gestures were found to be the most physically demanding. In general, methods that involved gestures (Gestures-only, GazeGestures, and GazeGestures+Random) were perceived to be more demanding.

4.6.4 Learning Effects. We also found that users authenticate faster as they enter more PINs, which suggests that there is a learning effect and that performance would eventually improve after repeated usage, i.e., GazeGestures+Random average results dropped from 56 seconds in the first attempt to 18 seconds in the last one.

Entry Time					
Significantly different Methods		$p <$	Significantly different Methods		$p <$
Gaze+Random (6.28 s)	Gestures-only (12.41 s)	0.001	Gestures-only (12.41 s)	GazeGestures+Random (20.63 s)	0.001
Gaze+Random (6.28 s)	GazeGestures+Random (20.63 s)	0.05	Gestures-only (12.41 s)	GazeGestures (19.43 s)	0.05
Gaze+Random (6.28 s)	GazeGestures (19.43 s)	0.001	Baseline (2.15 s)	Gaze+Random (6.28 s)	0.05
Gaze-only (5.31 s)	Gestures-only (12.41 s)	0.001	Baseline (2.15 s)	Gaze-only (5.31 s)	0.05
Gaze-only (5.31 s)	GazeGestures+Random (20.63 s)	0.01	Baseline (2.15 s)	Gestures-only (12.41 s)	0.05
Gaze-only (5.31 s)	GazeGestures (19.43 s)	0.001	Baseline (2.15 s)	GazeGestures (19.43 s)	0.05
			Baseline (2.15 s)	GazeGestures+Random (20.63 s)	0.05

Table 1: The baseline is significantly faster compared to the other methods. Gaze-only and Gaze+Random are significantly faster than all others except, Gaze+Random which is slightly slower than Gaze-only. Gestures-only is significantly faster than GazeGestures and GazeGestures+Random, while GazeGestures+Random is slightly slower than GazeGestures.



	Mental	Physical	Temporal	Performance	Effort	Frustration
Gaze Random	26.47	20.59	24.71	23.53	24.12	18.82
Gaze Fixed	21.76	15.59	21.18	18.53	20.88	21.76
Gestures	39.41	68.82	52.06	50.88	60.29	62.65
GazeGestures Random	73.82	58.53	55	52.35	67.06	61.47
GazeGestures Fixed	62.06	55.29	48.82	58.53	63.53	60.59
Basline	15.59	14.41	19.12	13.53	11.76	14.71

Figure 5: The mean Task Load index score of participants as indicated in the NASA TLX questionnaire.

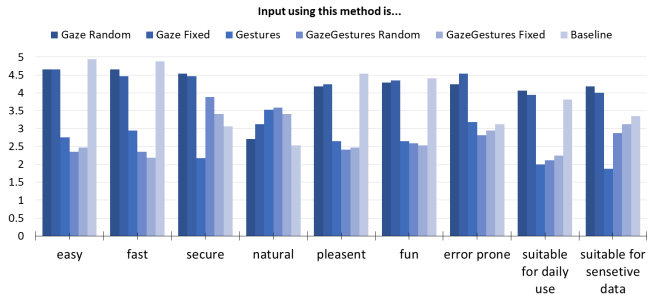


Figure 6: Qualitative feedback on the six methods on a 5-point Likert Scale (1 = Strongly Disagree; 5 = Strongly Agree).

4.6.5 Subjective Feedback. We collected subjective feedback through 5-point likert scale questions (see Figure 6), and held semi-structured interviews at the end of the study. Participants found Gaze-only and Gaze+Random particularly easy, fast, pleasant and fun compared to Gestures-only, GazeGestures, and GazeGestures+Random. They also indicated that they are more likely to use Gaze-only and Gaze+Random for their daily authentications. However, Gaze-only, GazeGestures and their variants were perceived to be more secure and likely to use to protect sensitive data. Participants rated Gestures-only negatively on almost all aspects. Participants rated Gaze-only and Gaze+Random as fun, easy and more secure than the Baseline. They found GazeGestures and GazeGestures+Random difficult to use but more secure. .

5 SECURITY STUDY EVALUATION

Since GazeGestures, Gaze-only and, Gestures-only are secure against smudge attacks and thermal attacks by design, we focused on evaluating and comparing the schemes in terms of observation resistance.

5.1 Apparatus and Participants

A 14" display (1366 × 768 pixels) was used in our experiments. We invited 16 participants (9 female), aged between 24 and 30 (Mean=24.68; SD=2.33), through word of mouth.

5.2 Experiment Procedure

Using the videos recorded in the usability study, each security study participant (attacker) performed two types of attacks: (1) Single-observation attack: the participant watched the video once and made up to three guesses against the password. This was done to simulate a case of casual observation, and (2) Video-observation attack: the participant had full control over the video and could pause and rewind as much as he/she likes. This was done to simulate a worst case scenario, where an attacker could record the user.

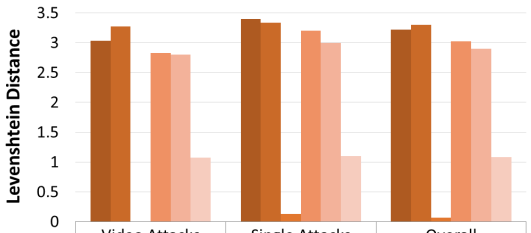
Each participant performed 12 single-observation attacks and 12 video-observation attacks. Note that we did not use all the videos that were recorded in the usability study. Instead, we used a random subset from the recordings such that a) each attacker observed an equal number of passwords entered using each input method through single-observations and two video-observations, and b) no attacker saw the same password more than once. After each attack, the participant could provide up to 3 guesses. Participants were provided with a pen and draft papers to take notes while performing the attacks.

Participants were not told if their guesses were correct before the end of the study to avoid biasing the reported perceived difficulty of observations. Participants were asked to put as much effort as possible and try their best to really find the entered passwords. The experiment took approximately 45 minutes.

After performing all attacks, the participants were asked to fill in a questionnaire (4 questions) in which they indicated on a 5-point Likert scale how easy it is to attack passwords and how confident they are about their answers for each password and attack type.

5.3 Experimental Design

Our study was conducted as a repeated measure experiment, where we had two independent variables: (1) the authentication method used in the previous study, and (2) the attack type: participants performed single observation attacks and video-observation attacks.



	Video Attacks	Single Attacks	Overall
Gaze Random	3.03	3.4	3.22
Gaze Fixed	3.27	3.33	3.3
Gestures only	0	0.13	0.07
GazeGestures Random	2.83	3.2	3.02
GazeGestures Fixed	2.8	3	2.9
Baseline	1.07	1.1	1.08

Figure 7: The lower the distance between the guess and the original PIN, the stronger the guess is.

5.4 Dependent Variables and Hypotheses

To evaluate the observation resistance, we measured the Levenshtein distance between the guesses and the correct password to analyze how close the guess is to the correct password. The Levenshtein distance refers to the distance between the attackers' guesses and the correct password; it is a commonly used metric in security analysis that reveals how close a guess is to the original password [13, 21, 25]. Thus, Levenshtein distance was the dependent variable.

The null hypothesis is:

$H_{1,0}$ There is no statistically significant relationship between the authentication method and Levenshtein distance.

5.5 Security Experiment Results

5.5.1 Levenshtein Distance. The mean Levenshtein distance per condition and per attack are illustrated in Figure 7. A repeated measures ANOVA with Greenhouse-Geisser correction revealed a significant main effect of authentication method on Levenshtein distance $F_{2.75,38.5} = 137.38$, $p < 0.001$; thereby disproving null hypothesis $H_{1,1}$. Pairwise comparisons with Bonferroni correction showed significant differences between baseline ($M = 1.08$, $SD = 0.16$) and all other conditions ($p < 0.001$), and between Gestures-only($M = 0.07$, $SD = 0.03$) and all other conditions ($p < 0.001$).

This means that guesses against PINs entered using Gestures-only are significantly closer to the correct PIN compared to guesses against PINs entered using the other methods (including the baseline). The second shortest distances to the original PINs were in case of guesses against Baseline, which were closer to the correct PIN compared to all other methods except Gestures-only. The lack of significant differences between the other methods means that we did not find any evidence that guesses against one of them are more successful than others.

5.5.2 Subjective Feedback. Figure 8, shows the collected subjective feedback from the participants. Attackers perceived Gestures-only to be easy to attack and were confident about their guesses in both attack types. This is comparable to the Baseline, where it has the second highest score in terms of easiness of attacks and the attackers' confidence. Gaze+Random is as easy to attack as GazeGestures, and attackers rated their confidence similarly too.

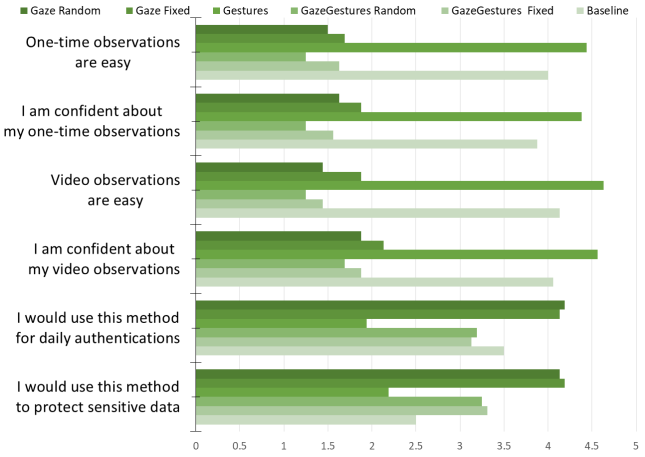


Figure 8: Participants rated their confidence in their attacks and their easiness on a Likert Scales (1 = Strongly Disagree; 5 = Strongly Agree).

The 2 methods are perceived to be more difficult than Gestures-only and Baseline. 7 participants rated Gaze-only as more difficult to attack compared to Gaze+Random and GazeGestures, and indicated that they are less confident about their guesses against them.

6 DISCUSSION

The results of the different evaluations allowed us to investigate the the usability and security of the authentication schemes.

6.1 Usability vs Security

Several works observed a trade-off between usability and security [12, 35]. Similarly, we also found such a trade-off. Although the usability of the GazeGestures (19.43s) and GazeGestures+Random (20.63s) are the lowest compared to all modalities, they offer higher security than the Baseline and Gestures-only. On the other hand, while Gestures-only (12.41s) has an adequate authentication time, it is error-prone and it is perceived to be the least secure.

In contrast, the Gaze-only and Gaze+Random achieve a balance between usability and security, where they have an adequate authentication time, the least error rate, and the least mental, physical, temporal, effort and frustration rates compared to GazeGestures, GazeGestures+Random, and Gestures-only. Gaze-only (5.31s) and Gaze+Random (6.28s) have the highest performance. They are also perceived to be the most secure against both attack types.

6.2 Iterative Attacks

Previous work evaluated multimodal authentication against iterative attacks, where the shoulder surfer attacks one modality per observation and then combines observations [21]. In our work, we evaluated the security schemes in a worst case scenario in which the attacker has access to a synchronized view of all necessary entities: the user's hand gestures, the user's eyes, and the on-screen number pad. In the usability study, we gathered information about the way users entered each PIN. For example, in the case of GazeGestures and GazeGestures+Random; we checked the combinations between

the digit entered by the gaze and the one entered by the hand, and whether the user uses the same combination every time they enter that digit (Stage 3 in the usability study). We found that most of the users (88%) use different combinations every time, and very few (12%) had their own pattern which they repeat.

This suggests that users would often enter the same PIN in different ways, which in turn means that performing iterative attacks is very less likely to succeed because the user might be performing different inputs by each modality each time. One example for this, a user could enter a 5 by gazing at 3 and extending 2 right-hand fingers, or by gazing at 4 and extending 1 right-hand finger.

6.3 Dominant and Non-Dominant Hands

We also found that participants tended to use a specific hand (mostly their dominant hand) in all cases unless they were asked to change it. However, they were annoyed by being forced to use a specific hand which was done in stage 4 for the GazeGestures and the GazeGestures+Random cases. In case of using the non-dominant hand, the authentication time was higher and more error-prone. Also, left-handed participants did not like that their left hand signaled subtractions. Thus in future systems should accommodate this. One way to accommodate this is to allow users to customize the use of each hand – this could also improve observation resistance as the attacker would need to know which configuration is being used.

For the Gestures-only modality, using both hands was very difficult for the participants as it required high physical and temporal demand, and that appeared in the TLX score (Figure 5). This led to a high score for Gestures-only in the frustration and effort level. The suggestion here is to use only one hand, however, this will reduce the number of possible combinations.

6.4 Effect of Randomized Layout

In contrast to our work, several previous works found a significant impact of randomized layout on security. For instance, users authenticated using GazeTouchPIN using gaze gestures in response to a randomized on-screen cue [24]. Similarly, in SwiPIN [34], random visual cues were shown on the digits to which users should swipe via touch accordingly. However, in our implementation we employed gaze dwell time, which is already more difficult to observe compared to gaze gestures and touch swipes. For this reason, the impact of the randomized layout is not apparent in our implementation. However, similar to previous work, the randomized layouts have a negative impact on usability. Therefore, since it negatively impacts usability and has a minor impact on security, we recommend refraining from using randomized layouts when using modalities that feature a high input entropy, such as gaze.

6.5 Guessing by Elimination

A disadvantage of GazeGestures is that attackers were able to sometimes guess PINs if the addition or the subtraction operations would otherwise result in a digit more than 9 or less than 0. For example, if a user gazes at 3 and extends 4 fingers but the attacker did not recognize which hand was used, the attacker could guess that the used hand was the right one since subtracting 4 from 3 would result in a number less than 0. This is a limitation in GazeGestures that ideally, users would keep in mind when using the technique.

6.6 Final Recommendations

To conclude, our results indicate that gaze-based authentication outperforms the other methods in terms of usability and security. We also argue that the random layout is not necessary; it increases authentication time but does not have a strong impact on security. Although a similar method was proposed in previous work [14], our implementation requires 5.3 second to authenticate, while previous work required 13 seconds.

Furthermore, the security evaluation shows that the method is highly resilient to shoulder surfing, while thermal and smudge attacks are unfeasible against gaze-based authentication by design. The fact that our implementation is not very different, yet the results are more positive than in the past, suggests that there is a need to revisit authentication schemes that were introduced in the past. Many introduced schemes were dismissed in practice due to requiring significantly longer entry times or due to high error rates. Nevertheless, our work demonstrates that the recent advances in visual computing offer more accurate sensors that can allow faster authentication times and lower error rates, while at the same time maintaining high resilience to shoulder surfing.

Gestures suffer from low usability and low observation resistance. Hence we do not recommend them for authentication.

Finally, GazeGestures demonstrate high security, albeit long authentication times and relatively high error rates. While observation resistance of Gaze-only was higher than that of GazeGestures, note that to attack GazeGestures the observer needs to simultaneously observe two views: the user's eyes, and the user's fingers. This means that in practice, attacking GazeGestures is more difficult. Furthermore, we believe that the continuously improving performance of eye trackers and motion sensors, and the observed learning effect promise better usability results in the future. Hence while GazeGesturesis not suitable for regular daily use, it can be suitable for highly sensitive contexts (e.g., when sensitive data is being accessed or when surrounded by shoulder surfers).

7 CONCLUSION AND FUTURE WORK

In this work, we introduced and evaluated 6 authentication schemes that employ gaze, gestures and multimodal combinations of them. We found that gaze offers a good balance between usability and security; it is highly secure against shoulder surfing yet requires shorter authentication times, and is less error-prone. Random on-screen layouts were found to negatively influence usability without a strong effect on security. Multimodal gaze and gestures show promise however with current technologies they are slow and error-prone, and in optimal conditions, it is worse in terms of observation resistance compared to gaze.

Future work should investigate different ways of integrating the proposed methods with biometric authentication. We also intend to investigate further threat models, such as insider attacks [37] and attacks from multiple observers [22].

REFERENCES

[1] Yomna Abdelrahman, Mohamed Khamis, Stefan Schneegass, and Florian Alt. 2017. Stay Cool! Understanding Thermal Attacks on Mobile-based User Authentication.

In *Proceedings of the 35th Annual ACM Conference on Human Factors in Computing Systems (CHI '17)*. ACM, New York, NY, USA. https://doi.org/10.1145/3025453.3025461

[2] Yasmeen Abdrabou, Mohamed Khamis, Rana Mohamed Eisa, Sherif Ismael, and Amr Elmougy. 2018. eNGAGE: Resisting Shoulder Surfing Using Novel Gaze Gestures Authentication. In *Proceedings of the 17th International Conference on Mobile and Ubiquitous Multimedia (MUM 2018)*. ACM, New York, NY, USA, 469–473. https://doi.org/10.1145/3282894.3289741

[3] Ilhan Aslan, Andreas Uhl, Alexander Meschtscherjakov, and Manfred Tscheligi. 2014. Mid-air Authentication Gestures: An Exploration of Authentication Based on Palm and Finger Motions. In *Proceedings of the 16th International Conference on Multimodal Interaction (ICMI '14)*. ACM, New York, NY, USA, 311–318. https://doi.org/10.1145/2663204.2663246

[4] Ilhan Aslan, Andreas Uhl, Alexander Meschtscherjakov, and Manfred Tscheligi. 2016. Design and Exploration of Mid-Air Authentication Gestures. *ACM Trans. Interact. Intell. Syst.* 6, 3, Article 23 (Sept. 2016), 22 pages. https://doi.org/10.1145/2832919

[5] Adam J. Aviv, Katherine Gibson, Evan Mossop, Matt Blaze, and Jonathan M. Smith. 2010. Smudge Attacks on Smartphone Touch Screens. In *Proceedings of the 4th USENIX Conference on Offensive Technologies (WOOT'10)*. USENIX Association, Berkeley, CA, USA, 1–7. http://dl.acm.org/citation.cfm?id=1925004.1925009

[6] Andrea Bianchi. 2011. Authentication on Public Terminals with Private Devices. In *Proceedings of the Fifth International Conference on Tangible, Embedded, and Embodied Interaction (TEI '11)*. ACM, New York, NY, USA, 429–430. https://doi.org/10.1145/1935701.1935815

[7] Andrea Bianchi, Ian Oakley, Vassilis Kostakos, and Dong Soo Kwon. 2011. The Phone Lock: Audio and Haptic Shoulder-surfing Resistant PIN Entry Methods for Mobile Devices. In *Proceedings of the Fifth International Conference on Tangible, Embedded, and Embodied Interaction (TEI '11)*. ACM, New York, NY, USA, 197–200. https://doi.org/10.1145/1935701.1935740

[8] Andrea Bianchi, Ian Oakley, and Dong Soo Kwon. 2012. Counting Clicks and Beeps: Exploring Numerosity Based Haptic and Audio PIN Entry. *Interact. Comput.* 24, 5 (Sept. 2012), 409–422. https://doi.org/10.1016/j.intcom.2012.06.005

[9] Alexander De Luca, Martin Denzel, and Heinrich Hussmann. 2009. Look into My Eyes!: Can You Guess My Password?. In *Proceedings of the 5th Symposium on Usable Privacy and Security (SOUPS '09)*. ACM, New York, NY, USA, Article 7, 12 pages. https://doi.org/10.1145/1572532.1572542

[10] Alexander De Luca, Alina Hang, Frederik Brudy, Christian Lindner, and Heinrich Hussmann. 2012. Touch Me Once and I Know It's You!: Implicit Authentication Based on Touch Screen Patterns. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI '12)*. ACM, New York, NY, USA, 987–996. https://doi.org/10.1145/2207676.2208544

[11] Alexander De Luca, Alina Hang, Emanuel von Zezschwitz, and Heinrich Hussmann. 2015. I Feel Like I'M Taking Selfies All Day!: Towards Understanding Biometric Authentication on Smartphones. In *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems (CHI '15)*. ACM, New York, NY, USA, 1411–1414. https://doi.org/10.1145/2702123.2702141

[12] Alexander De Luca, Marian Harbach, Emanuel von Zezschwitz, Max-Emanuel Maurer, Bernhard Ewald Slawik, Heinrich Hussmann, and Matthew Smith. 2014. Now You See Me, Now You Don't: Protecting Smartphone Authentication from Shoulder Surfers. In *Proceedings of the 32Nd Annual ACM Conference on Human Factors in Computing Systems (CHI '14)*. ACM, New York, NY, USA, 2937–2946. https://doi.org/10.1145/2556288.2557097

[13] Alexander De Luca, Emanuel von Zezschwitz, Laurent Pichler, and Heinrich Hussmann. 2013. Using Fake Cursors to Secure On-screen Password Entry. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI '13)*. ACM, New York, NY, USA, 2399–2402. https://doi.org/10.1145/2470654.2481331

[14] Alexander De Luca, Roman Weiss, and Heiko Drewes. 2007. Evaluation of Eye-gaze Interaction Methods for Security Enhanced PIN-entry. In *Proceedings of the 19th Australasian Conference on Computer-Human Interaction: Entertaining User Interfaces (OZCHI '07)*. ACM, New York, NY, USA, 199–202. https://doi.org/10.1145/1324892.1324932

[15] Heiko Drewes, Alexander De Luca, and Albrecht Schmidt. 2007. Eye-gaze Interaction for Mobile Phones. In *Proceedings of the 4th International Conference on Mobile Technology, Applications, and Systems and the 1st International Symposium on Computer Human Interaction in Mobile Technology (Mobility '07)*. ACM, New York, NY, USA, 364–371. https://doi.org/10.1145/1378063.1378122

[16] Malin Eiband, Mohamed Khamis, Emanuel von Zezschwitz, Heinrich Hussmann, and Florian Alt. 2017. Understanding Shoulder Surfing in the Wild: Stories from Users and Observers. In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems (CHI '17)*. ACM, New York, NY, USA, 11.

[17] Alain Forget, Sonia Chiasson, and Robert Biddle. 2010. Shoulder-surfing Resistance with Eye-gaze Entry in Cued-recall Graphical Passwords. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI '10)*. ACM, New York, NY, USA, 1107–1110. https://doi.org/10.1145/1753326.1753491

[18] Ceenu Goerge, Mohamed Khamis, Emanuel von Zezschwitz, Marinus Burger, Henri Schmidt, Florian Alt, and Heinrich Hussmann. 2017. Seamless and Secure VR: Adapting and Evaluating Established Authentication Systems for Virtual Reality. In *Proceedings of the Network and Distributed System Security Symposium (USEC '17)*. NDSS. https://doi.org/10.14722/usec.2017.23028

[19] Eiji Hayashi, Manuel Maas, and Jason I. Hong. 2014. Wave to Me: User Identification Using Body Lengths and Natural Gestures. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI '14)*. ACM, New York, NY, USA, 3453–3462. https://doi.org/10.1145/2556288.2557043

[20] Ponemon Institute. 2016. Global Visual Hacking Experimental Study: Analysis. multimedia.3m.com/mws/media/1254232O/global-visual-hacking-experiment-study-summary.pdf

[21] Mohamed Khamis, Florian Alt, Mariam Hassib, Emanuel von Zezschwitz, Regina Hasholzner, and Andreas Bulling. 2016. GazeTouchPass: Multimodal Authentication Using Gaze and Touch on Mobile Devices. In *Proceedings of the 2016 CHI Conference Extended Abstracts on Human Factors in Computing Systems (CHI EA '16)*. ACM, New York, NY, USA, 2156–2164. https://doi.org/10.1145/2851581.2892314

[22] Mohamed Khamis, Linda Bandelow, Stina Schick, Dario Casadevall, Andreas Bulling, and Florian Alt. 2017. They Are All After You: Investigating the Viability of a Threat Model That Involves Multiple Shoulder Surfers. In *Proceedings of the 16th International Conference on Mobile and Ubiquitous Multimedia (MUM '17)*. ACM, New York, NY, USA, 31–35. https://doi.org/10.1145/3152832.3152851

[23] Mohamed Khamis, Regina Hasholzner, Andreas Bulling, and Florian Alt. 2017. GTmoPass: Two-factor Authentication on Public Displays Using GazeTouch passwords and Personal Mobile Devices. In *Proceedings of the 6th International Symposium on Pervasive Displays (PerDis '17)*. ACM, New York, NY, USA, 9. https://doi.org/10.1145/3078810.3078815

[24] Mohamed Khamis, Mariam Hassib, Emanuel von Zezschwitz, Andreas Bulling, and Florian Alt. 2017. GazeTouchPIN: Protecting Sensitive Data on Mobile Devices Using Secure Multimodal Authentication. In *Proceedings of the 19th ACM International Conference on Multimodal Interaction (ICMI 2017)*. ACM, New York, NY, USA, 446–450. https://doi.org/10.1145/3136755.3136809

[25] Mohamed Khamis, Ludwig Trotter, Ville Mäkelä, Emanuel von Zezschwitz, Jens Le, Andreas Bulling, and Florian Alt. 2018. CueAuth: Comparing Touch, Mid-Air Gestures, and Gaze for Cue-based Authentication on Situated Displays. *Proc. ACM Interact. Mob. Wearable Ubiquitous Technol.* 2, 4, Article 174 (Dec. 2018), 21 pages. https://doi.org/10.1145/3287052

[26] Manu Kumar, Tal Garfinkel, Dan Boneh, and Terry Winograd. 2007. Reducing Shoulder-surfing by Using Gaze-based Password Entry. In *Proceedings of the 3rd Symposium on Usable Privacy and Security (SOUPS '07)*. ACM, New York, NY, USA, 13–19. https://doi.org/10.1145/1280680.1280683

[27] Keaton Mowery, Sarah Meiklejohn, and Stefan Savage. 2011. Heat of the Moment: Characterizing the Efficacy of Thermal Camera-based Attacks. In *Proceedings of the 5th USENIX Conference on Offensive Technologies (WOOT'11)*. USENIX Association, Berkeley, CA, USA, 6–6. http://dl.acm.org/citation.cfm?id=2028052.2028058

[28] Takashi Nagamatsu, Junzo Kamahara, Takumi Iko, and Naoki Tanaka. 2008. One-point Calibration Gaze Tracking Based on Eyeball Kinematics Using Stereo Cameras. In *Proceedings of the 2008 Symposium on Eye Tracking Research & Applications (ETRA '08)*. ACM, New York, NY, USA, 95–98. https://doi.org/10.1145/1344471.1344496

[29] Florian Schaub, Marcel Walch, Bastian Könings, and Michael Weber. 2013. Exploring the Design Space of Graphical Passwords on Smartphones. In *Proceedings of the Ninth Symposium on Usable Privacy and Security (SOUPS '13)*. ACM, New York, NY, USA, Article 11, 14 pages. https://doi.org/10.1145/2501604.2501615

[30] Ivo Sluganovic, Marc Roeschlin, Kasper B. Rasmussen, and Ivan Martinovic. 2016. Using Reflexive Eye Movements for Fast Challenge-Response Authentication. In *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security (CCS '16)*. ACM, New York, NY, USA, 1056–1067. https://doi.org/10.1145/2976749.2978311

[31] Chen Song, Aosen Wang, Kui Ren, and Wenyao Xu. 2016. "EyeVeri: A Secure and Usable Approach for Smartphone User Authentication". In *IEEE International Conference on Computer Communication (INFOCOM'16)*. San Francisco, California, 1 – 9.

[32] Martin Stokkenes, Raghavendra Ramachandra, and Christoph Busch. 2016. Biometric Authentication Protocols on Smartphones: An Overview. In *Proceedings of the 9th International Conference on Security of Information and Networks (SIN '16)*. ACM, New York, NY, USA, 136–140. https://doi.org/10.1145/2947626.2951962

[33] Furkan Tari, A. Ant Ozok, and Stephen H. Holden. 2006. A Comparison of Perceived and Real Shoulder-surfing Risks Between Alphanumeric and Graphical Passwords. In *Proceedings of the Second Symposium on Usable Privacy and Security (SOUPS '06)*. ACM, New York, NY, USA, 56–66. https://doi.org/10.1145/1143120.1143128

[34] Emanuel von Zezschwitz, Alexander De Luca, Bruno Brunkow, and Heinrich Hussmann. 2015. SwiPIN: Fast and Secure PIN-Entry on Smartphones. In *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems (CHI '15)*. ACM, New York, NY, USA, 1403–1406. https://doi.org/10.1145/2702123.2702212

[35] Emanuel von Zezschwitz, Alexander De Luca, Philipp Janssen, and Heinrich Hussmann. 2015. Easy to Draw, but Hard to Trace?: On the Observability of

Grid-based (Un)Lock Patterns. In *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems (CHI '15)*. ACM, New York, NY, USA, 2339–2342. https://doi.org/10.1145/2702123.2702202

[36] Emanuel von Zezschwitz, Paul Dunphy, and Alexander De Luca. 2013. Patterns in the Wild: A Field Study of the Usability of Pattern and Pin-based Authentication on Mobile Devices. In *Proceedings of the 15th International Conference on Human-computer Interaction with Mobile Devices and Services (MobileHCI '13)*. ACM, New York, NY, USA, 261–270. https://doi.org/10.1145/2493190.2493231

[37] Oliver Wiese and Volker Roth. 2016. See You Next Time: A Model for Modern Shoulder Surfers. In *Proceedings of the 18th International Conference on Human-Computer Interaction with Mobile Devices and Services (MobileHCI '16)*. ACM, New York, NY, USA, 453–464. https://doi.org/10.1145/2935334.2935388

[38] Xucong Zhang, Yusuke Sugano, Mario Fritz, and Andreas Bulling. 2015. Appearance-Based Gaze Estimation in the Wild. In *The IEEE Conference on Computer Vision and Pattern Recognition (CVPR)*.

[39] Yulong Zhang, Zhaonfeng Chen, Hui Xue, and Tao Wei. 2015. Fingerprints On Mobile Devices: Abusing and leaking. In *Black Hat Conference*.